NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

ENTERPRISE MOBILE DEVICE PRIVACY: HERE’S WHERE TO START

January 26, 2022

Organizations deploy mobile device solutions to address a variety of mission and business needs. Employees may use devices owned by the organization, commonly referred to as Corporate-Owned Personally-Enabled (COPE), or they may use their personal mobile devices to perform work-related activities, known as Bring Your Own Device (BYOD). The personal information that is processed as part of mobile device solutions, whether COPE or BYOD, introduces new privacy-related risks to the organization. While the idea of new privacy-related risks may sound daunting, these risks can be well managed through thoughtful risk analysis and design decisions resulting in more trust between employees and their organizations.

Privacy risks directly affect individuals and can cause issues to organizations as well. Both the individual and organizational implications of mobile device solutions should be considered when conducting a risk assessment.

Individual vs Organizational Privacy Concerns

Individuals directly experience privacy risk such as misuse of information.

In a mobile context, this could present itself as:

- Surveillance
- Unanticipated disclosure of information

Organizations can be impacted when causing privacy risks to individuals.

These impacts may include:

- Legal
- Financial
- Reputational

PRIVACY RESOURCES

To demonstrate how these privacy and organizational risks may be identified and addressed, the NCCoE applied several NIST tools when developing the COPE and BYOD example solutions. These tools and examples are intended to help practitioners conduct their own privacy risk analyses when deploying COPE and BYOD solutions within their respective mobile environments.

Below is a brief description of each tool and an example of how they were used in a mobile solution:

PRIVACY RISK ASSESSMENT METHODOLOGY (PRAM)

The PRAM applies the risk model from NIST Interagency Report (NISTIR) 8062 and helps organizations analyze, assess, and prioritize privacy risks to determine how to respond and select appropriate solutions.

PRAM Mobile Example

PRIVACY FRAMEWORK

The Privacy Framework is a voluntary enterprise risk management tool intended to help organizations identify and manage privacy risk and build beneficial systems, products, and services while protecting individuals' privacy.

Privacy Framework Mobile Profile Example

SPECIAL PUBLICATION (SP) 800-53, REVISION 5

NIST SP 800-53, Rev. 5 provides a consolidated catalog of security and privacy controls that address diverse requirements derived from mission and business needs, laws, executive orders, directives, regulations, policies, standards, and guidelines.

800-53 Controls Mobile Example

We are always interested in hearing from our communities of interest.
What privacy risks did you identify in your mobile device solutions, and how did you address them?
Your inputs may influence future mobile device projects at the NCCoE!

Please share with us by emailing mobile-nccoe@nist.gov.